UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/712,474	11/12/2003	Duc Pham	AESN3008CON1	9332

23488 7590 09/19/2007

GERALD B ROSENBERG
NEW TECH LAW
260 SHERIDAN AVENUE
SUITE 208
PALO ALTO, CA 94306-2009

EXAMINER	
DEBNATH, SUMAN	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
09/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/712,474	PHAM ET AL.	
	Examiner	Art Unit	
	Suman Debnath	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/23/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 June 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/23/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 are pending in this application.

2. Claims 1-2, 8, 12, 14, 17-18, 21, 25-27, 30 and 33-35 are presently amended in the amendment filed 23 May 2007.

Claim Objections

3. Claims 1, 8, 17, 25 and 30 are objected as failing to comply with the written description requirement. Claims recite limitation: "perform a non-sequential request for the transfer of a first predetermined sub-portion of a predetermined file stored by a network data store." "...with respect to the performance of said non-sequential request by enabling encrypted transfer of a second predetermined sub-portion of said predetermined file, inclusive of said first predetermined sub-portion, with respect to said network data store." The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Double Patenting

4. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140

F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 1-3, 5-20, 22, 24 and 30-35 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-9, 12, 19, 21-23 and 26-30 of U.S. Patent No. 6,678,828 B1, hereinafter "'828 application", issued to Pham et al. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following reasons:

6. Claim 1 of the instant application corresponds to claim 1 of '828 application, specifically in that the instant application is a broader characterization of the same invention.

7. Claim 2 of the instant application corresponds to claims 2 and 4 of '828 application, as follows: **authentication data includes user and session data (instant application);** authentication data defines a session with respect to the execution of said application program (claim 2 in '828 application); authentication data includes a verified user identifier (claim 4 in '828 application).

8. Claim 3 of the instant application corresponds to claim 12 of '828 applictaion, as follows: **authentication data includes a secure signature of said application program (instant application);** secure data protocol provides for the digital signing of the said first file data (claim 12 in '828 application).

9. Claim 5 of the instant application corresponds to claim 12 of '828 application, as follows: **generate a secure signature of said application program and provide said secure signature as part of said authentication data (instant application);** secure data protocol provides for the digital signing of said first file data (claim 12 in '828 application).

10. Claim 6 of the instant application corresponds to claim 8 of '828 application, specifically in that the instant application is a broader characterization of the same invention, as follows: **network appliance includes a policy parser operative to evaluate said authentication data and a policy data store including predetermined policy data accessible by said parser (instant application);** network appliance further includes an access policy store which stores a plurality of predetermined access policies, and wherein said network appliance is operative to qualify said file data request against said plurality of predetermined access policies stored by said access policy store (claim 8 in '828 application).

11. Claim 7 of the instant application corresponds to claim 9 of '828 application.

12. Claim 8 of the instant application corresponds to claims 1 and 8 of '828 application, specifically in that the instant application is a broader characterization of the same invention.

13. Claim 9 of the instant application corresponds to claim 4 of '828 application, as follows: **authentication data includes an authenticated identification of a user associated with said application program (instant application);** authentication data includes a verified user identification (claim 4 of '828 application).

14. Claims 10, 11, 12 and 14 of the instant application corresponds to claims 2, 12, 21 and 5 of '828 application, respectively.

15. Claim 13 of the instant application corresponds to claim 26 of '828 application, specifically in that the instant application is a broader characterization of the same invention.

16. Claim 15 of the instant application corresponds to claims 6 and 7 of '828 application, as follows: **policy data store further provides for the storage of an encryption key identifier determinable by said policy parser on evaluation of said file request message (instant application);** network appliance provides for the

storage of meta-data, including an encryption key identifier, in correspondence with said predetermined network file and wherein said network appliance provides for the retrieval of said meta-data (claim 6 of '828 application); **network appliance obtains an encryption key identified by said encryption key identifier for use in the cipher processing of file data transferred in connection with said modified file request (instant application);** network appliance includes an encryption key store and wherein said encryption key identifier selects an encryption key provided to said encryption unit in connection with said second file data request (claim 7 of '828 applictaion).

17. Claims 16, 17, 18, 19, 20, 22, 24 of the instant application corresponds to claims 8, 19, 3, 4, 22, 23, 19 of '828 application, respectively. Specifically in that the instant application is a broader characterization of the same invention.

18. Claim 30 of the instant application corresponds to claims 26 and 30 of '828 application, specifically in that the instant application is a broader characterization of the same invention.

19. Claim 31 of the instant application corresponds to claims 27 and 28 of '828 application, specifically in that the instant application is a broader characterization of the same invention.

20. Claim 32, 33, 34 and 35 of the instant application corresponds to claim 29 of '828 application.

Claim Rejections - 35 USC § 103

21. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

22. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Graham et al. (Pub. No.: US 2002/0178271 A1) (hereinafter "Graham") and further in view of Peters et al. (Patent No.: US 6,374,336 B1) (hereinafter "Peters").

23. As to claim 1, Graham discloses a network storage architecture supporting securely controlled access and bidirectional transfer of data between a client computer system and a network data store (FIG. 1, [0064], [0090], "...the proxy file management system supports both read and write file operation"), said network storage architecture comprising:

a) an agent program ([0064], lines 11-14, client module reads on agent program), executed on a client computer system (FIG. 1, item 150), and operative with respect to an application program ([0128], lines 1-4), to develop authentication data with respect to said application program (FIG. 4, [0128]), wherein said application program, as executed by said client computer system, is operative to perform a request for the

transfer of a first predetermined file stored by a network data store, said authentication data including a representation of request ([0021], [0065], [0095], [0107]); and

b) a network appliance, coupleable through a communications network to said client computer system (FIG. 1, proxy system 110, [0067], lines 1-10), interoperable with said agent program to receive and validate said authentication data ([0066], line 2-11, as describes the proxy system which determines if the requesting user has the right to access the file reads on receiving and validating the authentication data), said network appliance determining selectively to control execution of said application program ([0066], lines 7-11) with respect to the performance of said request by enabling encrypted transfer of a second predetermined file, inclusive of said first predetermined portion, with respect to said network data store ([0092], [0093], [0106], "The natively supported NFS protocol is used to access and modify the NAS file system").

Graham doesn't explicitly disclose wherein request wherein client computer system perform a non sequential request for the transfer a first predetermined sub-portion of file; network appliance control execution of non-sequential request by enabling transfer of second predetermined sub-portion of predetermined file.

However, Peters discloses wherein request wherein client computer system perform a non sequential request for the transfer a first predetermined sub-portion of file (col. 2, lines 52-60); network appliance control execution of non-sequential request by enabling transfer of second predetermined sub-portion of predetermined file (col. 2, lines 52-67 to col. 3, lines 1-17 and col.4 lines 36-44).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Graham as taught by Peters in order to make efficient data transfer by optimizing bandwidth utilization on a network storage.

24. As to claim 2, Graham discloses that the authentication data includes user and user session data ([0160], lines 1-4, lines 6-8, Graham teaches the concept of including user and session data as part of authentication data by identifying the entity with whom the server and client are communicating and by ensuring the live-ness, i.e., the current session as part of authentication service).

25. As to claim 3, wherein said authentication data includes a secure signature of said application program ([0216]-[0217], Graham teaches of generating a secure signature by including a signature flag that indicates the payload has been signed by the source).

26. As to claim 4, Graham discloses the agent program operative to obtain user authentication and collect data with respect to user sessions and processes to develop said authentication data ([0128], line 1-4)

27. As to claim 5, Graham discloses that the agent program is further operative to generate a secure signature of said application program and provide said secure

signature as part of said authentication data ([0216]-[0217], Graham teaches of generating a secure signature by including a signature flag that indicates the payload has been signed by the source).

28. As to claim 6, Graham discloses a policy parser operative to evaluate said authentication data (FIG. 3, item 226, [0101], lines 6-12, The management service modules reads on the policy parser) and a policy data store including predetermined policy data accessible by said policy parser (FIG. 3, policy database 370, [0115], lines 1-4).

29. As to claim 7, Graham discloses that the predetermined policy data, as evaluated by said policy parser, is determinative of said response message ([0107], lines 7-11).

30. As to claim 8, Graham discloses a network storage architecture supporting securely controlled access and bidirectional transfer of data between a client computer system and a network data store (FIG. 1, [0064], [0090]), said network storage architecture comprising:

a) an agent program ([0064], lines 11-14, client module reads on agent program), executed on a client computer system (FIG. 1, item 150), responsive to a source file request issued with respect to a network data store by an application program executed by said client computer system ([0118], lines 8-12), wherein a source file is stored by said network data store ([0106]) and wherein said source file request is a read/write

request specifying transfer of a first defined said source file ([0092], [0093], [0106]), said agent program being operative to develop authentication data with respect to said application program ([0128], lines 1-4, authentication service module is operative as part of client module, e.g., see FIG. 4) and to provide a file request message including a representation of said source file request and said authentication data ([0065], lines 9-14); and

b) a network appliance, coupleable through a communications network to said client computer system (FIG. 1, proxy system 110, [0067], lines 1-10) and responsive to said file request message ([0066], lines 7-11), said network appliance including a policy parser operative to evaluate said file request message (FIG. 3, item 226, [0101], lines 6-12, The management service modules reads on the policy parser) and a policy data store including predetermined policy data accessible by said policy parser (FIG. 3, policy database 370, [0115], lines 1-4), said network appliance, responsive to the evaluation of said file request message ([0107], lines 7-11), enabling performance of said source file request with respect to said network data store ([0106], lines 3-8) including transfer from said network data store a second defined portion of said source file inclusive of said first defined portion of said source file ([0092], [0093], [0106], "The natively supported NFS protocol is used to access and modify the NAS file system").

Graham doesn't explicitly disclose source file request is a random read/write request for the transfer a first defined sub-portion of source file; network appliance control execution of non-sequential request by enabling transfer of second defined sub-portion of source file.

However, Peters discloses source file request is a random read/write request for the transfer a first defined sub-portion of source file (col. 2, lines 52-60); network appliance control execution of non-sequential request by enabling transfer of second defined sub-portion of source file (col. 2, lines 52-67 to col. 3, lines 1-17 and col.4 lines 36-44).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Graham as taught by Peters in order to make efficient data transfer by optimizing bandwidth utilization on a network storage.

31. As to claim 9, Graham discloses the authentication data includes an authenticated identification of a user associated with said application program ([0128], lines 1-4, FIG. 4).

32. As to claim 10, Graham discloses the authentication data includes user session and context data ([0160], lines 1-4, lines 6-8, Graham teaches of including user session and context data as part of authentication data by identifying the entity with whom the server and client are communicating and by ensuring the live-ness, i.e., the current session as part of authentication service).

33. As to claims 11, Graham discloses that the authentication data includes a secure signature of said application program ([0213], lines 2-6, [0217], which describes a

signature flag that indicates the payload has been signed by the source reads on including a secure signature).

34. As to claim 12, Graham discloses the network appliance that enables generation of a modified file request corresponding t said source file request and direct to said network data store ([0106], lines 3-8, FIG. 1, Graham inherently teaches the generation of modified file request in order to pass the request from client 150 to proxy system 110 then to network storage 160 by supporting NFS protocol which is used access and modify the NAS file-system).

Graham doesn't explicitly disclose said modified file request specifying transfer of said second defined sub-portion of said source file. However, Peters discloses a file request specifying transfer of a second defined sub-portion of a source file (col. 2, lines 52-67 to col. 3, lines 1-17 and col.4 lines 36-44).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Graham as taught by Peters in order to make efficient data transfer by optimizing bandwidth utilization on a network storage.

35. As to claim 13, Graham further discloses comprising a first communications network through which said file request message is received by said network appliance ([0067], lines 1-10) and a second communications network through which said modified file request is provided to said network data store ([0080], lines 9-14).

36. As to claim 14, Graham discloses wherein said network appliance includes an encryption unit ([0092], lines 1-3, Graham teaches of using an encryption engine within the content subsystem; [0066], lines 7-11, Graham teaches of including an encryption unit by providing the file in an encrypted manner) and wherein said network appliance further provides for the cipher processing of said source file as transferred in connection with said modified file request ([0204], lines 1-3, encryption key is provided for the cipher processing of file data transfer) such that said source file is encrypted as transferred to said network data store ([0092]).

Graham doesn't explicitly disclose processing of first and second defined sub-portion of a source file. However, Peters discloses processing of first and second defined sub-portion of a source file (col. 2, lines 52-67 to col. 3, lines 1-17 and col.4 lines 36-44).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Graham as taught by Peters in order to make efficient data transfer by optimizing bandwidth utilization on a network storage.

37. As to claim 15, Graham discloses wherein said policy data store further provides for the storage of an encryption key identifier determinable by said policy parser on evaluation of said file request message ([0093], lines 5-13) and wherein said network appliance obtains an encryption key identified by said encryption key identifier for use in

the cipher processing of file data transferred in connection with said modified file request ([0204], Graham teaches of obtaining an encryption key identified in order to deliver the encryption key).

38. As to claim 16, Graham further discloses wherein said authentication data includes a process identifier ([0118], lines 1-2), corresponding to said application program as executed on said client computer system ([0118], lines 8-12), a verified user identifier ([0160], lines 1-4), and a group identifier (page 13, table 1, lines 26-29), and wherein said policy parser is operative to qualify said file request message against said predetermined policy data with respect to said process identifier, verified user identifier, and group identifier ([0179], lines 1-3).

39. Claims 17-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Graham and further in view of Blumenau et al. (Patent No.: US 6,845,395 B1) (hereinafter "Blumenau").

40. As to claim 17, Graham discloses a method of securing access by a client computer system to file data stored on a storage device accessible by said client computer system ([FIG. 1), said method comprising the steps of:

a) intercepting, by a first program ([0064], lines 11-14, client module reads on first program) as executed on a client computer system (FIG. 1, item 150, [0140], client module filter driver, [0141], lines 1-3), a data transfer request issued by a second

program, as executed on said client computer system ([0144], lines 9-13, the application reads on the second program), directed to a data file stored by a client accessible file data store ([0064], lines 1-5; and [0139], lines 12-15);

b) first processing, by said first program, said data transfer request to associate authentication data with said data transfer request ([0128], lines 1-4);

c) evaluating, by a security appliance coupled to said client computer system through a communications network (FIG. 1, proxy system 110, [0067], lines 1-10), said data transfer request, said authentication data, and access control data corresponding to said data file to qualify said data transfer request ([0101], lines 6-12, [0093], lines 5-13); and

d) second processing to selectively enable said data transfer request to proceed relative to said data file dependent on the qualification of said data transfer request ([0140], lines 8-14);

Graham doesn't explicitly disclose wherein said data transfer request specifies transfer of a first sub-portion of said data file to said client accessible file data store; second processing including the steps of i) retrieving a second sub-portion of said data file; ii) decrypting said second sub-portion; iii) incorporating said first sub-portion into said second sub-portion; iv) encrypting said second sub-portion and v) transferring said second sub-portion to said client accessible file data store for incorporation into said data file.

However, Blumenau discloses wherein said data transfer request specifies transfer of a first sub-portion of said data file to said client accessible file data store (col.

1, lines 55-61, col. 6, lines 28-35, col. 7, lines 45-67, "...the source ID filed 52 of the packet to index into configuration data identifying which of the volumes of data the respective host has privilege to access); second processing including the steps of i) retrieving a second sub-portion of said data file (col. 6, lines 28-35, col. 7, lines 45-67); ii) decrypting said second sub-portion (col. 12, lines 51-65 and col. 13, lines 60-67); iii) incorporating said first sub-portion into said second sub-portion (col. 12, lines 51-65 and col. 13, lines 60-67); iv) encrypting said second sub-portion col. 12, lines 51-65 and col. 13, lines 60-67 () and v) transferring said second sub-portion to said client accessible file data store for incorporation into said data file (col. 6, lines 29-35, col. 7, lines 45-57, col. 12, lines 51-65 and col. 13, lines 60-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Graham as taught by Blumenau in order to "allow the control of the data management to be centralized in one location, rather than distributed throughout the network. Centralizing the data management control at the storage system removes the need to trust the hosts seeking access to the storage system to only access certain portions of data. (Blumenau, col. 5, lines 35-45)"

41. As to claim 18, Graham discloses the authentication data includes process ([0118], lines 1-2) and context identification information ([0175]).

42. As to claim 19, Graham discloses the authentication data includes a verified user identifier ([0160], lines 1-4) and a process identifier ([0118], lines 1-2).

43. As to claim 20, Graham further discloses the authentication data includes a verified user identifier ([0160], lines 1-4), a process identifier ([0118], lines 1-2), a group identifier (Table 1, lines 26-29).

44. As to claim 21, Graham discloses wherein said data file includes file data that, as stored by said client accessible file data store, is stored as a plurality of discretely encrypted blocks, wherein said first and second sub-portions of said data file are respectively first and second sub-portions of the file data of said data file, wherein said data transfer request specifies a data range of file data ([0141], lines 13, [0106]) and wherein said second processing step includes the step of modifying said data range to correspond to a sub-plurality of said discretely encrypted blocks defining said second sub-portion, thereby accommodating the block encryption of file data within said data file ([0141], lines 1-7, [0092]).

45. As to claim 22, Graham discloses wherein said step of evaluating associates encryption control data with said data transfer request ([0141], lines 4-7) and wherein said second processing step, responsive to said encryption control data, includes cipher processing of file data transferred in connection with said data transfer request ([0141],

lines 7-10, Graham teaches of including cipher processing by delivering the file in an encrypted format).

46. As to claim 23, Graham further discloses the steps of: a) first transferring said data transfer request to said security appliance through a first communications network ([0067], lines 1-10); and b) second transferring said data transfer request relative to said client accessible file data store through a second communications network ([0080], lines 9-14).

47. As to claim 24, Graham discloses that the security appliance is established a network portal through which network file accesses are routed between said client computer system and said client accessible file data store (FIG. 1, [0065], lines 9-14, Graham teaches the concept of establishing a network portal by providing the proxy system as a function of information which coupled with authentication system and policy system and with end-user client device through communication network in order to provide access to the network storage).

48. As to claim 25, Graham discloses a method of securing file access operations by a client computer system made with respect to a client accessible file data store (FIG. 1), said method comprising the steps of:

a) intercepting, by a first program ([0064], lines 11-14, client module reads on first program) executing on a client computer system (FIG. 1, item 150, [0140], client

module filter driver, [0141], lines 1-3), file operation requests issued by a second program, as executing on said client computer system ([0144], lines 9-13, the application reads on the second program), wherein said file operation requests are issued with respect to files selectively stored encrypted in a filesystem accessible by said client computer system ([0064], lines 1-5; and [0139], lines 12-15, [0092]);

b) determining, by said first program relative to a predetermined file operation request, authentication data for said second program ([0128], lines 1-4), wherein said authentication data includes user and process identification data ([0160], lines 1-4, lines 6-8) and a representation of said predetermined file operation request ([0217]);

c) enabling, by a security appliance responsive to said authentication data (FIG. 1, proxy system 110, [0067], lines 1-10; and [0143], lines 1-2), said predetermined file operation request with respect to a file identified by said predetermined file operation request ([0175], lines 1-3), wherein said enabling step is dependent on qualification ([0101], lines 6-12, [0093], lines 5-13), by said security appliance (FIG. 1, proxy system 110), of said authentication data against policy data defining operation permissions relative to said file including a write operation permission to allow modification of said file as stored encrypted in said filesystem ([0101], lines 6-11; and [0140], lines 8-14, [0090], [0165], [0183]);

Graham doesn't explicitly disclose d) transferring predetermined encrypted blocks of file data representing a sub-portion of said file in response to said predetermined file operation request through a network connection where said

predetermined encrypted blocks of file data are decrypted, modified, encrypted, and returned through said network connection for storage as part of said file.

However, Blumenau discloses d) transferring predetermined encrypted blocks of file data representing a sub-portion of said file in response to said predetermined file operation request through a network connection where said predetermined encrypted blocks of file data are decrypted (col. 6, lines 29-35, col. 7, lines 45-57, col. 12, lines 51-65 and col. 13, lines 60-67), modified, encrypted, and returned through said network connection for storage as part of said file (col. 6, lines 29-35, col. 7, lines 45-57, col. 12, lines 51-65 and col. 13, lines 60-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Graham as taught by Blumenau in order to "allow the control of the data management to be centralized in one location, rather than distributed throughout the network. Centralizing the data management control at the storage system removes the need to trust the hosts seeking access to the storage system to only access certain portions of data. (Blumenau, col. 5, lines 35-45)"

49. As to claim 26, Graham further discloses a method of securing file access operations includes the steps of:

a) associating an encryption key with said predetermined file operation request determined from the qualification of said authentication data against said policy data ([0093], lines 5-13, [0101], lines 6-12); and

b) cipher processing, using said encryption key, said predetermined encrypted blocks of file data transferred relative to said file ([0066], lines 7-11, cipher processing is done in order to provide the file in a secure and encryption manner).

50. As to claim 27, Graham discloses wherein said predetermined file operation includes a specification of file data to be transferred and wherein said step of cipher processing includes modifying said specification of said predetermined file operation request to correspond to said predetermined encrypted blocks of file data transferred relative to said file ([0141], lines 1-7).

51. As to claim 28, Graham discloses the step of cipher processing is performed on said security appliance ([0092], lines 1-3; [0141], lines 7-10).

52. As to claim 29, Graham discloses authentication data includes a verified user identification ([0160], lines 1-4) and a login process identification ([0142], lines 4-12).

53. As to claim 30, Graham discloses a security appliance (FIG. 1, proxy system 110) for securing bidirectional access by client computer systems to persistently stored remotely encrypted data files (FIG. 1, [0090]), said security appliance comprising:

a) a processor coupleable to a client computer system to receive an access request message ([0064], lines 11-14, client module reads on processor), wherein said access request message includes authentication data ([0128], lines 1-4) and an

identification of a read/write file data transfer operation directed to an identified data file stored encrypted in a persistent data file store ([0217], [0090], [0165], [0183], [0349]); and

b) a policy data store (FIG. 3, policy database 370, [0115], lines 1-4), accessible by said processor, providing for the storage of predetermined file operation qualifiers applicable to data files present in said persistent data file store ([0175], lines 1-3), wherein said policy data store is maintained secure by said processor with respect to said client computer system (FIG. 1, proxy system 110, [0107], lines 7-11), and wherein said processor is operative to selectively enable said read/write file data transfer operation dependent on an evaluation of said predetermined file operation qualifiers with respect to said access request message ([0101], lines 6-12; and [0140], lines 8-14, [0090], [0165], [0169], [0183]);

Graham doesn't explicitly disclose random data transfer; access request message to transfer an encrypted sub-portion of said identified data file through a network connection for remote decryption, modification and return through said network connection for storage as part of said identified data file.

However, Blumenau discloses random data transfer; access request message to transfer an encrypted sub-portion of said identified data file through a network connection for remote decryption, modification and return through said network connection for storage as part of said identified data file (col. 6, lines 29-35, col. 7, lines 45-57, col. 12, lines 51-65 and col. 13, lines 60-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Graham as taught by Blumenau in order to "allow the control of the data management to be centralized in one location, rather than distributed throughout the network. Centralizing the data management control at the storage system removes the need to trust the hosts seeking access to the storage system to only access certain portions of data. (Blumenau, col. 5, lines 35-45)"

54. As to claim 31, Graham discloses the authentication data includes a verified user identifier ([0160], lines 1-4) and a group identifier (page 13, table 1, lines 26-29) and wherein said processor is operative to discriminate said verified user identifiers, said group identifier, said file operation and said identified data file against said predetermined file operation qualifiers to obtain said evaluation ([0101], lines 6-12).

55. As to claim 32, Graham discloses that the policy data store further provides for the storage of encryption keys in association with said predetermined file operation qualifiers ([0093], lines 5-13) and wherein said processor is operative to retrieve a predetermined encryption key from said policy data store dependent on said evaluation ([0204], Graham teaches the concept of retrieving an encryption key in order to deliver the encryption key).

56. As to claim 33, Graham discloses wherein said processor, responsive to said evaluation, is further operative to provide for said file operation to be passed through said network connection to said persistent data file store ([0106], lines 3-8).

57. As to claim 34, Graham discloses wherein said processor, responsive to said evaluation, is further operative to modify a specification of said read/write file data transfer operation to encompass the transfer of said encrypted identified data file the performance of said read/write file data transfer operation with respect to said identified data file ([0141], lines 1-4, [0090], [0165]).

Graham doesn't explicitly disclose random file data transfer operation to encompass the transfer of sub-portion of data. However, Blumenau discloses random file data transfer operation to encompass the transfer of sub-portion of data (col. 6, lines 29-35, col. 7, lines 45-57, col. 12, lines 51-65 and col. 13, lines 60-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Graham as taught by Blumenau in order to "allow the control of the data management to be centralized in one location, rather than distributed throughout the network. Centralizing the data management control at the storage system removes the need to trust the hosts seeking access to the storage system to only access certain portions of data. (Blumenau, col. 5, lines 35-45)"

58. As to claim 35, Graham discloses wherein said processor includes an encryption engine operative to process said encrypted data file as transferred through said network connection ([0092], lines 1-3, Graham teaches of using an encryption engine within the content subsystem).

Graham doesn't explicitly disclose processing of sub-portion of said identified data file. However, Blumenau discloses processing of sub-portion of said identified data file (col. 6, lines 29-35, col. 7, lines 45-57, col. 12, lines 51-65 and col. 13, lines 60-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Graham as taught by Blumenau in order to "allow the control of the data management to be centralized in one location, rather than distributed throughout the network. Centralizing the data management control at the storage system removes the need to trust the hosts seeking access to the storage system to only access certain portions of data. (Blumenau, col. 5, lines 35-45)"

59. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part

of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Response to Amendment

60. Applicant has amended claims 1-2, 8, 12, 14, 17-18, 21, 25-27, 30 and 33-35, which necessitated new ground of rejections. See rejection above.

Response to Arguments

61. In response to file a terminal disclaimer to over come Double Patenting rejection, no terminal disclaimer was filed. Therefore, Double Patenting rejection stands.

62. Applicant argues that: "Graham which discloses a read only, file at a time only content distribution system does not identically teach the present invention as set forth in Claim 1."

Examiner has carefully reviewed Applicant's argument and maintains that Graham processes read/write request operation of data file and processes multiple packets (i.e. portion of a file at a time) as part of a request (e.g. see, FIG. 6A, 7, [0090], [0165], [0169], [0183], [0349]).

Conclusion

63. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

64. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD
SD

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100